



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/753,727	01/03/2001	Rosario Gennaro	RSW920000091US1	3760

7590 03/04/2005  
Gerald R. Woods  
IBM Corporation T81/503  
P.O. Box 12195  
Research Triangle Park, NC 27709

EXAMINER

HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 03/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No. 09/753,727	Applicant(s) GENNARO, ROSARIO	
	Examiner Matthew T Henning	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --.

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 04 November 2004.
- 2a) ☒ This action is FINAL.      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-7, 9-19, 21-32, 34-37, 39-45 and 47 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-7, 9-19, 21-32, 34-37, 39-45 and 47 is/are rejected.
- 7) ☒ Claim(s) 5-6, 17-18, and 29-30 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 03 January 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |   |   |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

Art Unit: 2131

This action is in response to the communication filed on 11/04/2004.

### **DETAILED ACTION**

1. All rejections and objections not set forth below have been withdrawn.
2. Claims 1-7, 9-19, 21-32, 34-37, 39-45, and 47 have been examined.
3. Claims 8, 20, 33, 38, and 46 have been cancelled.

#### ***Title***

4. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: *Method, Apparatus, and Computer Program Product for Generating Pseudo-Random Bits.*

#### ***Priority***

5. No claim for priority has been made for this application.
6. The effective filing date for the subject matter defined in the pending claims in this application is January 03, 2001.

#### ***Information Disclosure Statement***

7. The information disclosure statement (IDS) submitted on 01/03/2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

#### ***Drawings***

8. The drawings filed on 01/03/2001 are acceptable for examination proceedings.

*Claim Objections*

9. Claims 5-6, 17-18, and 29-30 are objected to for failing to comply with the standard claim numbering as set forth in 37 CFR 1.75(c).

10. The applicant is reminded that a series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

A claim which depends from a dependent claim should not be separated by any claim which does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

*Claim Rejections - 35 USC § 102*

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

*A person shall be entitled to a patent unless –*

*(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.*

12. Claims 13-19, 21-22, 24-33, 34-35, and 37, 39-45, and 47 are rejected under 35 U.S.C. 102(b) as being anticipated by Patel et al (“An Efficient Discrete Log Pseudo Random Generator”) hereinafter referred to as Patel.

13. Claim 13 recites a system for efficiently generating pseudo-random bits in a computing environment, comprising: means for providing an input value (See Patel Page 313 Section 5 Line 10); means for generating an output sequence of pseudo-random bits (See Patel Page 313 Section

Art Unit: 2131

5 Lines 11-12) using the provided input value as input to a 1-way function (See Patel Page 313 Section 5 Line 10 wherein the function  $x_{i+1} = g^x \bmod p$  is one-way) wherein a length in bits, C (See Patel Page 316 Lines 1-11,  $\omega(\log n)$ ), of the input value is substantially shorter than a length in bits, N (See Patel Page 316 Lines 1-11,  $x_{i+1}$ ), of the generated output sequence (See Patel Page 307 Problem 2), and means for using C selected bits of the generated output sequence as the provided input value for the next iteration of the means for generating while using all N-C remaining bits of the generated output sequence as pseudo-random output bits (See Patel Page 316 Lines 1-11), until a desired number of pseudo-random output bits have been generated (See Patel Page 316 Lines 1-11, wherein the feedback is performed for all  $i > 0$ ).

14. Claim 14 recites that the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption (See Patel Page 307 Section 2.1).

15. Claim 15 recites that the 1-way function is modular exponentiation modulo a safe prime number (See Patel Page 313 Section 5 Line 10 and Page 307 Paragraph 6 Lines 7-8).

16. Claim 16 recites that the input value is used as an exponent of the modular exponentiation (See Patel Page 313 Section 5 Line 10).

17. Claim 17 recites that a base of the modular exponentiation is a fixed generator value (See Patel Page 304 Section 1 Lines 3-4).

18. Claim 18 recites that the length of the input value is 160 bits (See Patel Section 2.1 Lines 1-2 wherein x is the input of 160 bits) and a length of the safe prime number is 1024 bits (See Patel Page 307 Lines 5-6).

19. Claim 19 recites that the length of the input value is at least 160 bits (See Patel Section 2.1 Lines 1-2 wherein x is the input of 160 bits) and the length of the generated output sequence

Art Unit: 2131

is at least 1024 bits (See Patel Abstract Lines 11-13 wherein n is the number of bits output by the generator prior to bit extraction as disclosed by Patel in Section 6).

20. Claim 21 recites that the  $N - C$  remaining bits are concatenated to pseudo-random output bits previously generated by the means for generating (See Patel Abstract and Section 7.1).

21. Claim 22 recites that the  $N - C$  remaining bits are selected from the  $N$  bits of the generated output sequence as a contiguous group of bits (See Patel Section 7.1 Lines 3-4).

22. Claim 24 recites means for using the desired number of generated pseudo-random output bits as input to an encryption operation (See Patel Page 305 Lines 15-17).

23. Claims 25-30 are rejected for the same reasons as claims 13-18 above.

24. Claims 31-32 are rejected for the same reasons as claim 19 above.

25. Claims 34-35 are rejected for the same reasons as claims 21-22 above.

26. Claim 37 is rejected for the same reasons as claim 24 above.

27. Claim 39 is rejected for the same reasons as claims 13 and claim 24 above.

28. Claims 40-45, and 47 are rejected for the same reasons as claims 14-19, and 21 above.

### ***Claim Rejections - 35 USC § 103***

29. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

*(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.*

Art Unit: 2131

30. Claims 23, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patel as applied to claims 13 and 25 respectively above, and further in view of Schneier ("Applied Cryptography").

Patel disclosed selecting a set of bits from the output as the new input (See rejection of claim 20 above), but failed to disclose that the bits were selected in a non-contiguous manner.

Schneier teaches that in order to reach a maximal period for a pseudo-random bit generator, the feedback bits should be a primitive polynomial mod 2 (See Schneier Page 374 lines 9-20, and further shows an example of this type of feedback (See Schneier Page 375 Figure 16.4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier to the pseudo-random bit generator of Patel in order to provide primitive polynomial mod 2 feedback to the generator. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide the longest period for the generator to ensure the most produced bits before cycling.

31. Claims 1-7, and 9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patel, and further in view of Schneier ("Applied Cryptography").

Regarding claim 1, Patel disclosed a system for efficiently generating pseudo-random bits in a computing environment, comprising: means for providing an input value; means for generating an output sequence of pseudo-random bits using the provided input value as input to a 1-way function wherein a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence, and means for using C selected bits of the generated output sequence as the provided input value for the next iteration of the means for

Art Unit: 2131

generating while using all N-C remaining bits of the generated output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated (See rejection of claim 13 above), but Patel failed to disclose that this system was implemented in software. However, Patel did disclose that these pseudo-random bits were for encryption (See Patel Page 305 Lines 15-17).

Schneier teaches that any encryption algorithm can be implemented in software and that doing so helps with flexibility and portability, ease of use, and ease of upgrade (See Schneier Page 225 Paragraph 7 Lines 1-3). Schneier further teaches that software encryption programs are popular (See Schneier Page 225 Paragraph 8 Line 1).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the pseudo-random number generator of Patel by implementing the generator in software. This would have been obvious because the ordinary person skilled in the art would have been motivated to improve the portability, ease of use, and ease of upgrade of the generator.

32. Claims 2-7, and 9-12 are rejected for the same reasons as claim 14-19, and 21-24 above, as applied to claim 1.

### ***Response to Amendment***

33. In response to the amendment to the title of the invention, the examiner feels that the title as amended is even less descriptive than the original, and is therefore maintaining the objection to the title.

### ***Conclusion***

34. Claims 1-7, 9-19, 21-32, 34-37, 39-45, and 47 have been rejected.



Art Unit: 2131

35. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Patel et al. (U.S. Patent Number 6,285,761) disclosed a pseudo-random bit generator based on the assumption known as "discrete logarithms with short exponents".

36. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

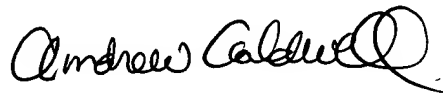
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Matthew Henning  
Assistant Examiner  
Art Unit 2131  
2/24/2005



**ANDREW CALDWELL**  
**SUPERVISORY PATENT EXAMINER**